What is Chainlink VRF?

Blockchains for instance Bitcoin are dealing with a fundamental issue. The issue is of spreading the decisive consensus fairly, which also concerns the pool of winning the competition. The issue is also of having the authority to add a new block to the blockchain along with the probability of winning.

Modern cryptography has gone to its best extent to solve this issue. A way to solve this problem is by drawing out randomly, which works in a decentralized mechanism. This implication of the cryptographic lottery is known as the Verifiable Random Function (VRF).

What is VRF?

VRF stands for Verifiable Random Function, is defined as the public key. This public key is the version of a hash that is keyed cryptographic. The hash can only be computed by the holder of the private key. Irrespective of the ownership of the private key, anyone with an access to the private key can validate the authenticity of the hash. VRFs help in the prevention of hash-based data structures' enumeration. The functioning of smart contracts is supported by the VRF in case of randomness.

Let's understand the concept of VRF along with Chainlink, how does Chainklink VRF works and supports the smart contracts in blockchain in the further sections.

Possible Attacks with the Randomness Approach

In the Ethereum ecosystem, every node tries to solve the issue and check the transaction. After all the nodes verify the issues, they broadcast them to the entire network. For instance, we develop a dApp where the coin is flipped by us with the head as the winning side.

The above function is used to obtain the prediction of heads and tails. If you wish to run a node, you can publish transactions only to your node, and it will not be shareable. You will run the randMod function, or you can also flip the coin until you have only shared the transaction after you have won.

One way to resolve this issue is the implication of oracle to get access to a random number function that is not a part of the Ethereum blockchain. You can also go through different cryptographic algorithms and function of the third party which can be used but are not safe and needs to be audited.

Chainlink VRF stands for Chainlink Verifiable Random Function, which is a proven and verified link of randomness precisely curated for smart contracts. Developers using smart contracts can take the assistance of Chainlink VRF, as it helps them with a tamper-proof RNG to create safe, smart contracts for various applications. These applications depend on varied, unpredictable results as mentioned below:

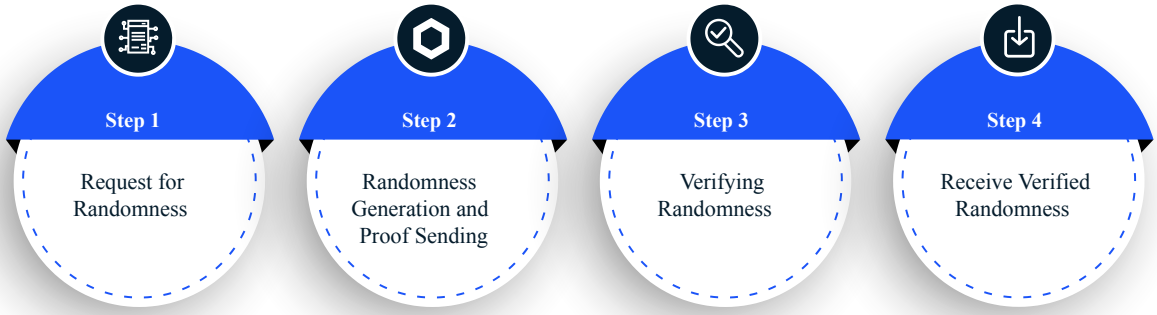
- NFTS and different blockchain games
- Randomly assigning duties and resources
- Selection of representative sample concerning the mechanism of consensus

Every time a new request for random outcome pops up, the Chainlink VRF creates a random number and proof that is cryptographic in nature, stating the determination of the number. The proof generated is then verified and published on-chain before it gets utilized by other consuming applications. This proof generation process ensures that the data cannot be tampered with or altered by anyone for their benefit. With Verifiable Random Function (VRF) assistance, developers creating smart contracts can develop different games with more security with the assistance of a source of randomness that is verified on-chain. This also allows the developers to give added proof to the security-sensitive users.

Now let’s understand how the Chainlink VRF works while deploying a smart contract on a blockchain platform.

How does Chainlink VRF work?

Working Mechanism of Chainlink VRF



LeewayHertz

Chainlink Verifiable Random Function works by supporting smart contracts. Let's understand the steps of the Chainlink VRF mechanism in the below-mentioned points:

- When the smart contracts are deployed, it gives a hint to the network of Chainlink Oracle requesting a random number.
- This hint cannot be predicted by the oracle and will be utilized to create a random number. Every oracle ensures the use of its private key to create random numbers.
- Once the results and proofs get published on-chain, oracle's public key and a hint of the smart contract can be utilized for authentication.
- This process leverages the benefit of the popular verification attribute of the blockchain platform.
- The contracts can specifically use random numbers that have already been checked and authenticated in a similar blockchain ecosystem.
- The major advantage of working with a Chainlink VRF while deploying smart contracts is that the random numbers can be checked.
- Even if a node gets attacked, the node cannot manipulate or change the final result because it cannot pass the encryption check on the chain.
- The worst case is that the down node does not respond to the request, which will be recorded by the blockchain immediately and then will stay on the chain forever.
- Users can query valid tests and no longer use nodes that fail to respond or provide valid signature records.
- Even if the node is operated, the final random number generated will not be affected. Busy nodes can only choose not to respond to requests.
- Under the next chainlink delivery mechanism, this behavior will be fined, and the problem node will be removed from the list of random number generators. Therefore, illegal or low-quality nodes will suffer huge economic losses in the short and long term.
- In short, as long as the chain link VRF is connected properly, it can never be tampered with. The only thing that can possibly occur is that the problem node is offline or unresponsive, and then it is completely eliminated. This mechanism gives great security for smart contract developers and users.

The advantage of the VRF chain is that, as the number of users increases, the cost that users pay to node operators will increase accordingly, so nodes will be more motivated to provide the highest possible security. After that, users can request encryption security through gambling and pay more for additional security. In this way, paying users will form a global shared resource pool, and users who should have spent money to develop their own RNG solutions will use this money to improve the security level of shared resources in the entire blockchain ecosystem.

Chainlink has been connected to blockchains such as Polkadot and tezos, which means that the users of the Chainlink ecosystem will form a network effect and continue to expand, and the number of users and encryption security levels will also form a complementary virtuous circle.

Why should we use Chainlink VRF?

There are some distinctive features of the Chainlink VRF that makes it an essential in the blockchain.

- It regulates the process of Random Number Generation (RNG) for the smart contracts.
- Chainlink VRF produces unbiased randomness for the game outcome.
- Consuming smart contracts get all the random number results after they are verified.
- With Chainlink VRF, oracles cannot manipulate the result generated.
- Providing users the integrity of the game along with the cryptographic proof, which builds a trust level.
- Chainlink VRF does not allow the malicious users and the node operators to alter and tamper with the randomness results.

What are the technical specifications of Chainlink VRF?

Chainlink VRF is the application of Goldberg Verifiable Random Function (VRF). The term Random in 'Verifiable Random Function' defines any entity not having a hint or key and cannot predict at any cost. This explains the mechanism of the uniform probability distribution.

The technical specifications of the Chainlink VRF are as follows:

- The VRF has a key that is encrypted by the Oracle machine.
- In contrast to the VRF key, oracle has a public key corresponding to it.
- Oracle then binds its corresponding public key with the VRF key and the ID of the chainlink task present on-chain.
- During the process, when a smart contract is requesting a random number, it gives a seed.
- To make sure that the results of the VRF cannot be guessed, it is important to store the unpredictable and difficult to alter with the values in the seed.

- For instance, the recent block hash value or the chain data that is verified and encrypted.
- VRF amalgamates the smart contract seed with different data to steer clear of the replay attacks and give some fundamental security for the contract with specific additional protection.
- Once the VRF present on the chain has done the determination of a seed, it will then continue requesting the corresponding VRF results as required by a smart contract from oracle by broadcasting in Ethereum log.

Let's understand the mechanism of Chainlink VRF with its use cases.

Use Cases of Chainlink VRF

- **Unbias Gaming Outcomes**
  Users get the lottery smart contract, which proves that the winners are selected with only random data. This random data can be verified by people on-chain. Users get the assurance and surety to involve themselves in the smart contract and have confidence in the fact that they enjoy a winning probability. For instance, Pooltogether is a capital verified deposit lottery game on Ethereum. It is a principal secured savings game, which collects the user's deposits together, initiates a lottery daily or every week, and pays the deposit interest as a bonus to the winner. The game encourages users' saving behavior through a lottery mechanism.
  Pooltogether takes the assistance of chainlink VRF to create verifiable random numbers, which can demonstrate to its users that each issue's winners are chosen by absolute random numbers. Along with their security assurance, it also ensures to users that the key hints and the security of the key links are traceable, and the process of random number generation can be checked thoroughly.
- **Secure NFT Distribution**
  You can use chainlink VRF to reward distinct non-fungible tokens and ascertain the crate contents for the selling items with the help of your supply schedule. This will also allow the players to get an access to the auditable proof supporting their NFT backed assets' creation done with tamper-proof randomness.
  For instance, Wildcards have used Chainlink VRF to enrich the randomness experience in their ecosystem to become the epitome of animal conservation worldwide.
- **Engaging Player Experiences**
  With the help of Chainlink VRF, you can also increase the experience of uncertain environments and unpredictable scenarios. Yet you will be able to fetch out the compatible mix in strategy and fun to ascertain the outcomes in battles of PvP and other dynamic scenarios.
  For instance, Facegolf uses the Chainlink VRF to get a randomness solution that is secure and on-chain. With this, they avoid the expose of their future users to all sorts of malicious activities that they had faced in the past.

Conclusion

The network of Chainlink Oracle has more than 1000 nodes which are of premium quality. With the help of threshold signature technology, the network becomes efficiently scalable and decentralized in nature in a cost-effective manner. This will provide a supreme level of decentralization and availability to Chainlink VRF. With the growing need to deploy smart contracts in the blockchain ecosystem, chainlink VRF gives a secure way of generating random numbers for easy probability in various domains of gaming.

Contact our smart contract developers to get an in-depth and realistic understanding of the Chainlink VRF.